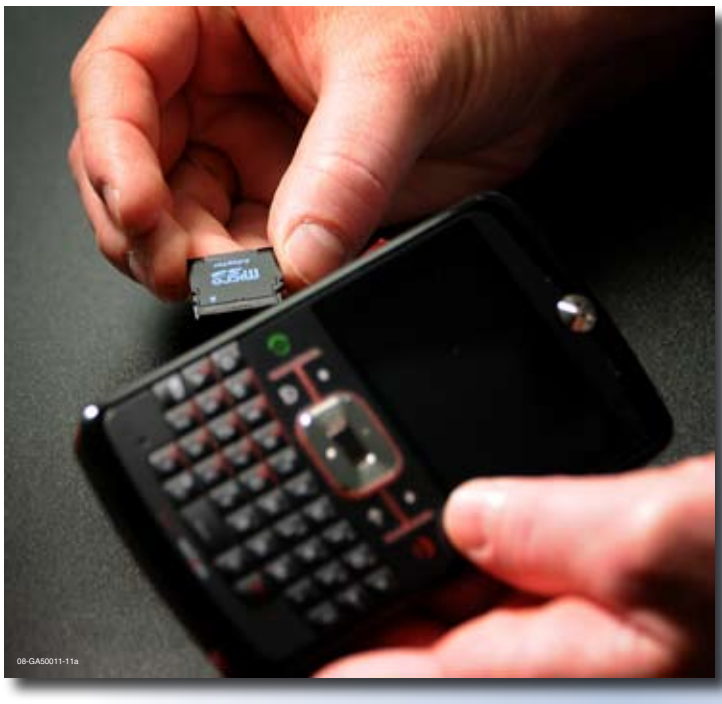
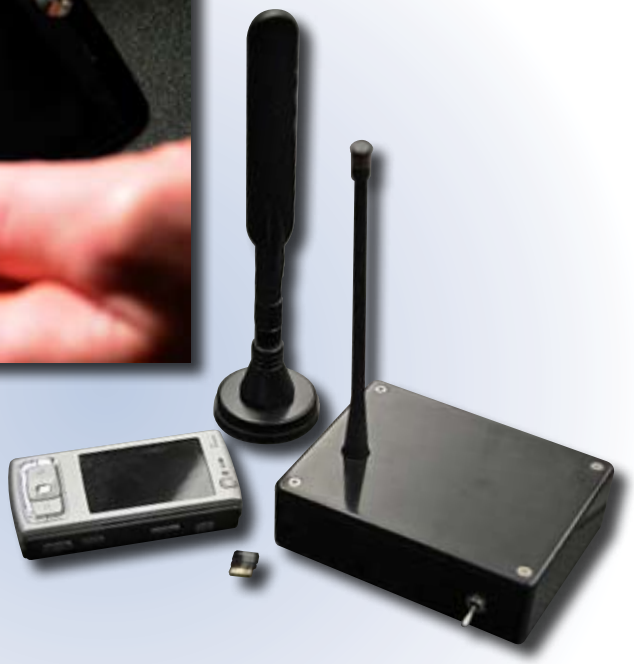




Wireless Sentinel can be deployed as a Micro-SD card with RFID or can be integrated into device hardware. It uses an antennae for detecting and interrogating Sentinel-enabled phones.

Wireless Sentinel

Securing Wireless Business Devices

As smart phones become electronic wallets, securing daily transactions is a must.

An INL research team designed the ultimate security solution, called the Wireless Sentinel, ensures totally secure, encrypted wireless communications and financial transactions. The system also secures designated use areas – detecting unauthorized cell phones and permitting only authorized wireless devices to operate in the zone.

This security system consists of a physical processing module located at one or more nodes on a wireless network, and software operating within a wireless communications device (e.g. a smart phone) that encrypts communication with wireless networks. The Wireless Sentinel can be designed into wireless device hardware or be installed as a micro-Secure Digital (micro-SD) card with radio frequency identification found on current- and next-generation wireless devices.

No Snooping Allowed

Impressively, encryption is performed in a secure and protected memory chip, which isolates its internal processes from snooping. The secure encryption system prevents the device from decrypting the communication and secures the device physically and wirelessly from hacks, intercepts or attacks.

Even more impressive, is that the Wireless Sentinel detects cell phone break-ins and reports suspicious changes in the phone's operating system to its network. Identification and authentication software is installed on each device that creates and archives a

Continued next page

Continued from previous page

signature of key information including unique identification numbers, known operating system states, and software settings. When the access control system detects any wireless device within its monitored area – it actively interrogates the device, which must respond with the proper authentication credentials – or it determines that the system has been modified without authorization.

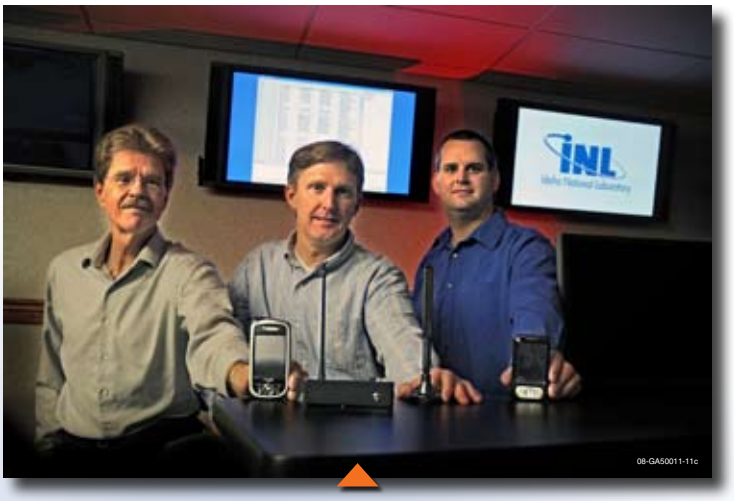
Enabling Secure m-Commerce

Just as Internet security technology made electronic shopping and banking possible, the Wireless Sentinel system will unleash the power of cell phone based m-Commerce, which Juniper Research predicts will grow to $63 billion worldwide by 2010. Another $103 billion per year is predicted in social money markets for entertainment, dinners and cab fares. This conversion to m-Commerce is a reality in Europe and Asia.

The first viruses specifically targeting cell phones began to emerge in 2004. As smart phones are used to conduct more and more transactions today, information theft and malicious tampering become serious threats. Without Wireless Sentinel, these threats could impede the emergence of robust m-Commerce.

Thwarting Information Theft, Espionage

The proliferation of cell phone technology is adding to the growing challenge of industrial and government espionage. The American Society for Industrial Security estimates that espionage costs Fortune 1000 companies more than $53 billion a year. According to the 2004 annual report to Congress on Foreign Economic Collection and Industrial Espionage, such espionage costs the U.S. economy from $100 to $250 billion annually.



Wireless Sentinel provides industries concerned with cell phone-based espionage a method of keeping unauthorized cell-phones out of sensitive areas without hindering the use of these business-critical devices by authorized users like the CEO.

Cell phones can be easily triggered remotely to become eavesdropping devices. In response, governments and corporations often ban wireless devices from sensitive areas. While this addresses security, it limits productivity and hinders access to business-critical communications.

Wireless Sentinel enrolls an organization's wireless devices into an access control system and discovers devices attempting to enter controlled areas. By authenticating wireless devices approved for entry into sensitive areas (e.g., corporate boardroom or high-security areas), an organization can allow their use while simultaneously discovering and disallowing non-approved devices.

When a phone within wireless range of the Wireless Sentinel system is unauthorized or has been compromised, the Wireless Sentinel alarm system is triggered. The security application of the system can be configured differently for corporations, military or m-Commerce users. For Wireless Sentinel systems installed for national or corporate security purposes, detection of a compromised or unauthorized cell phone would activate an alert to physical security officers or surveillance systems.

For more information

Technical Contacts

Steven H. McCown
208-526-2373
Steven.McCown@inl.gov

Technology Transfer Contact

Charity Follett
208-526-9353
Charity.Follett@inl.gov

A U.S. Department of Energy National Laboratory